Pulse

Comes to You 2009

IBM

Managing the World's Infrastructure

Managing risk during acquisitional growth

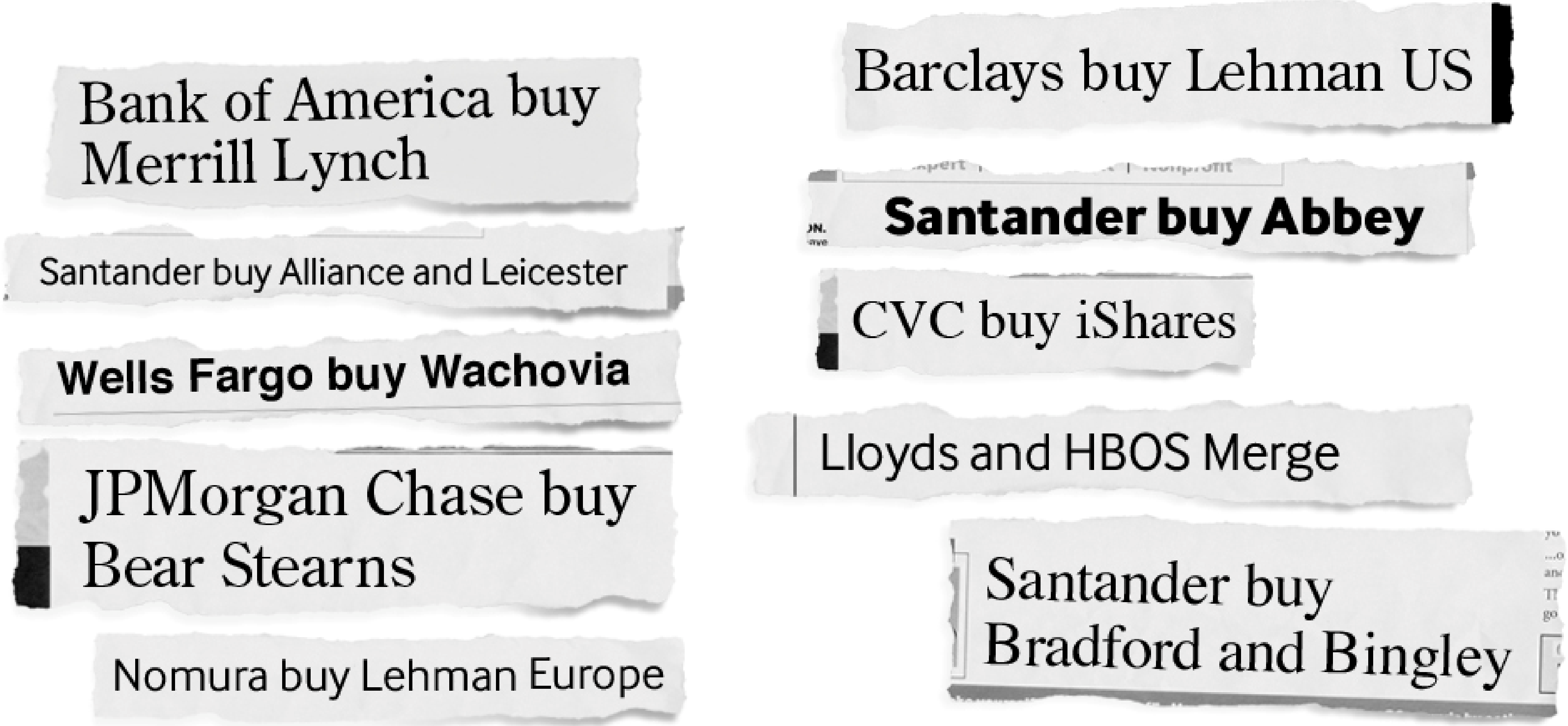
Mike Cartwright, Pirean, 19th May 2009

IT Governance

- IT Governance is the ability of IT to deliver services, as well as looking to establish and enforce controls within which the business must operate.
- Service Delivery must respond to the demands of the organisation, whilst balancing services in line with the assessment and management of risk.

Managing Organisational Risk

- Risk planning is strongly centred on the experience and knowledge within an organisation.
- Organisational risk can be mitigated by providing more detailed and business relevant information.
- Issues over the past few years have exposed the shortfall in availability of the information required to analyse and contain risk.
- In today’s turbulent climate – change is moving at an unprecedented pace...



Bank of America buy Merrill Lynch

Santander buy Alliance and Leicester

Wells Fargo buy Wachovia

JPMorgan Chase buy Bear Stearns

Nomura buy Lehman Europe

Barclays buy Lehman US

Santander buy Abbey

CVC buy iShares

Lloyds and HBOS Merge

Santander buy Bradford and Bingley

Identity Lifecycle Management

- Organisations recognise the need to establish a best practice framework around the management of identities within the enterprise.

- Solutions must align with regulatory compliance, best practice, and existing IT administration controls.

- There are significant challenges in managing identities across disparate systems.

Current Economic Climate

- Processes for managing Joiners, Movers and Leavers need to be tightly managed.

- Employees leaving the organisation need their access rights tightly managed, and they need to be de-provisioned quickly.

- Temporary workers save on labour costs and provide increased flexibility.
  - Normally come with a high turnover rate
  - No detailed history or control over future positions in the organisation
  - Keeping track of access is not easy

Current Economic Climate

- As well as being faced with increased demand for accountability and requirements to demonstrate control, the current economic climate is not helping.

- Re-organisations, Mergers and rationalisation have a major impact on IT administration.

- IT Administration is often one of the key areas targeted for cut backs.

Mergers / Acquisitions

- The number of Applications under management can increase dramatically overnight.

- Visibility of access permissions across the organisation reduces dramatically.

- Managers are made responsible for individuals, with rights over unfamiliar applications.

- No individual has a complete understanding of the IT Estate.

- Audit requirements remain.

Pulse

Comes to You 2009

Managing the World's Infrastructure

Key Security challenges during major change

Key Challenges for Security during acquisitions & mergers. .

1. Managing the challenges of Identity

   Who has access?

   What Access do they have?

   What specialist skills are required to understand and validate access in these times of change?

   How do we audit and report on compliance?

   Who has access across organisations?

Key Challenges for Security

2. Quickly on-boarding and managing new services and changing business units

Provisioning Access quickly, but with control and auditability

Hardening new Data Centres and systems

Ensuring services are secured and compliant with Corporate Policy

Key Challenges for Security

3. Delivery and securing of new customer facing services

    Provisioning Services provided to customers will change, ideally levering the best solutions from within each of the organisations

    We need a continued focus on Continuity and Service Assurance

    The number of services, and array of silo based approaches to security, can cause significant increases in complexity and workload – there is a real need for a standard approach to application security

    The opportunity is presented to implement a central shared service for managing and provisioning access

The right combination of process, procedure and technology is key

1. Managing the challenges of Identity

   IBM Tivoli Identity Manager

2. Quickly on-boarding and managing new services and changing business units

   IBM Tivoli Access Manager for Operating Systems
   IBM Tivoli Compliance Insight Manager
   IBM Tivoli Security Operations Manager

3. Delivery and securing of new customer facing services

   IBM Tivoli Access Manager for e-Business

... and whilst going through this programme, take time to strengthen controls and improve the end user experience

IBM Tivoli Access Manager provides one secure key to the door;

With **Enterprise Single Sign-On** for improved user experience;

and **IBM Tivoli Identity Manager** for centralised Identity Management;

and reduced support costs through Identity Management User Self-Service.

Pulse

Comes to You 2009

IBM

Managing the World's Infrastructure

Common challenges in Governance and Risk Management

Some common GRC challenges we see today . . .

1. Provide the business with the information they need to make key decisions regarding risk

2. Providing a view of access in a business context

3. Make the business responsible and accountable for compliance. Remove some of the burden from the Security Teams, through improved delegation and increased automation

4. Derive audit centric value from the identity and access data within the Tivoli solution

Some common key challenges

5. Demonstrate to an auditor that we have controls and good practice in place

6. Demonstrate a long term commitment through adherence to process

7. Provide business orientated reports on identity and access

8. Address Orphan Account Management

9. Deliver a Segregation of Duties solution (A.K.A. Separation)

Case Study 2 – Major High Street Bank Addressing SOx Compliance

Project Timeline

February 2007 Bank select IBM and Pirean to perform a pilot of IBM Tivoli Identity Manager (ITIM) and Pirean’s own Segregation of Duties enhancement for ITIM.

June 2007 On successfully completing the pilot, IBM and Pirean are selected to deliver a bank wide programme for Logical Access Management.

December 2007 IBM Tivoli Identity Manager, IBM Directory Integrator and a customised Console are deployed in production.

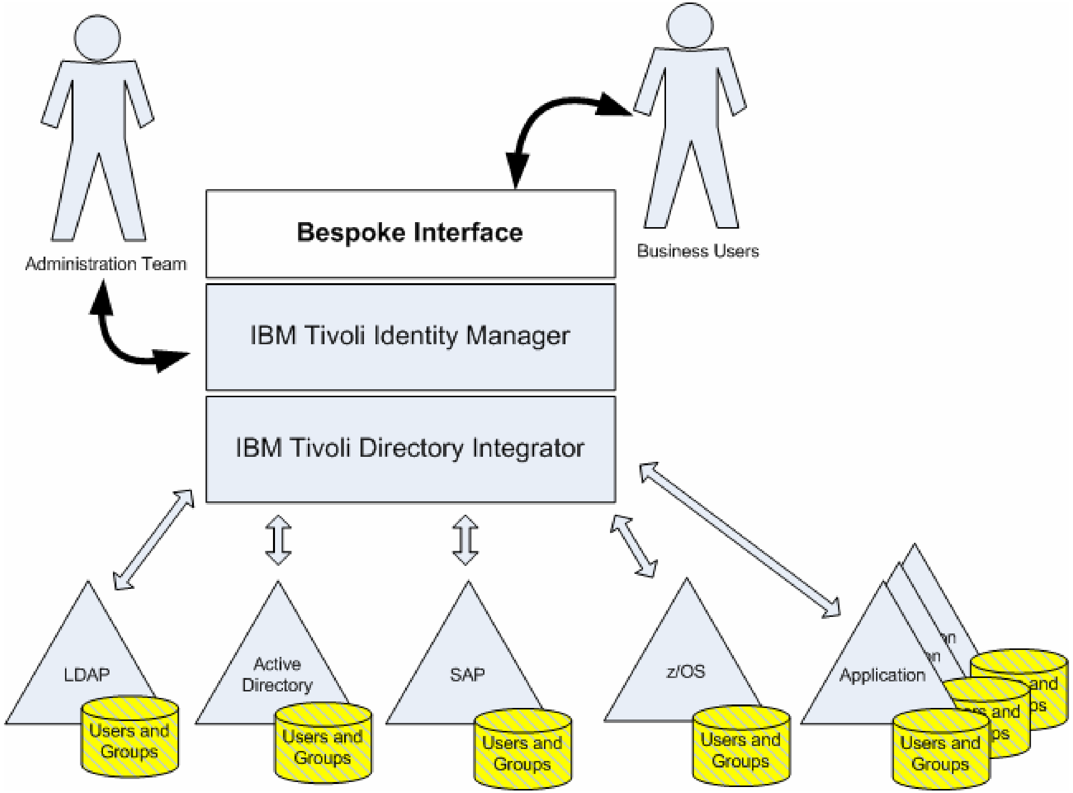
March 2008 After the successful business pilot of the solution, Bank engages IBM and Pirean to deliver enhanced functionality for the ITIM implementation and Console .

August 2008 The next generation Console for the administration for Logical Access controls is born and deployed in Banks’ production environment.

December 2008 After the successful business pilot, IBM Tivoli Software is managing the Banks Group’s identities and SOX critical applications

February 2009 Throughout 2009, the bank have engaged in the continued roll out across Business Critical applications

Solution Implementation



Business Focused Interface

- Customers want to pass the day to day management of accounts back to the business.

- Improved audit and control through enabling managers to easily administer their teams and their access privileges.
  - You are accountable
  - You can regularly review your team and their access
  - You have a published task list of all other actions (for example, managing compliance breaches)

- We automated business processes through workflow - from line manager approval of new access privileges to the transfer of an employee to their team.

Access recertification

- Access recertification, allows an organisation to improve their understanding of who has access to what and why.
- We provide an interface to enable and assist business users to perform these functions. Managers and their delegates are required recertify their teams access – and are accountable for their decisions.
- Automated, scheduled recertification cycles, combined with e-mail notification, work queues and workflow realise the solution.

Orphan Account Management

- Companies recognise that users should not logon as root – and that users actions should be accountable.
- From a security Audit perspective - every account needs an owner or custodian.
- The task of processing all accounts, on all systems, can be labour intensive and time consuming.

Orphan Account Management

- Managing all accounts from a central location enables us to apply logic to identify account owners.
- We make Application Owners responsible for Orphan Accounts, requesting they identify the owner, assign a custodian, or remove the account.
- Business Application owners are provided with a GUI to assist in locating owners and creating the relationships.
- We provide daily reports on Orphan Accounts – and a complete audit history.

Segregation of Duties

- Most IT organisations have basic, manual methods to ensure that users don’t get conflicting rights within an application.

- Few have any way to detect conflicts between entitlements across applications.

Segregation of Duties

- As part of the solution we implemented a SoD compliance engine, enabling complex combinations of permissions to be tested across people, applications and platforms.

- The solution manages compliance across more than 50 applications and 150,000 users.

- Through Workflow we enable compliance breach management - providing options for dispensation management.

- This results in reduced risk and improved compliance - removing the risk of unauthorised access privileges.

Audit and Reporting

- Applications containing sensitive information need to be audited for compliance.

- Auditors want to know :
- How did a user gain access and why ?
- Who approved their access and when ?
- Is their access regularly reviewed and approved?
- What is the history of their access, what changes have been made over time and who authorised them?

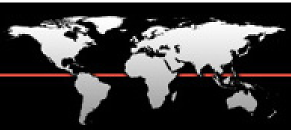
- Repeatedly answering these questions through manual reviews is both time-consuming and expensive.

Case Study

- The solution as described is an example of Tivoli Identity Management software currently deployed in a Major UK Bank.

- The same solution is currently being tailored to address the compliance requirements of a Pathfinder Local Authority.

- The solution currently under review with an additional three UK Banks.



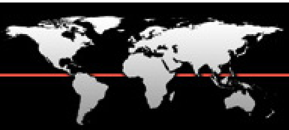
Case Study 2 – Another Major High Street Bank Access Management

Challenge.

- This Major Bank had recently acquired another bank – and all of its applications and infrastructure.

- They had a large number of bespoke applications, from both organisations, each with a slightly different approach to access management and control.

- Acquisition brought a change in staff, skill sets, roles and responsibilities – as well as a the challenge of understanding the systems that support key services.



Challenge.

- The Bank identified the cost of training staff to support these different solutions was high.
- They acknowledged that their model needed to change from ‘Build in house’ to Buy.
- They wanted the capability to control Access from one place.
- They wanted to standardise on One Model – embracing Access, Audit and Compliance.
- They recognised the need for longevity and flexibility to embrace new technologies.
- They embraced the principle of a single solution for access management.

Solution.

- IBM and Pirean Technology was implemented to deliver a centralised login infrastructure which protects back-end applications.

- Branded to reflect the corporate image.

- Providing the Access layer to all backend applications and services.

Solution.

- A single logon application - centrally managed access control.
- Built on Tivoli Access Manager for eBusiness, the solution is proven to scale to support thousands of users, extendable on a project by project basis.
- Adaptable to support the requirements of all backend applications.
- A central point to rapidly enable the adoption of new technologies.
- One Model – embracing Access, Audit and Compliance.

Questions ?

www.pirean.com/ComplianceOne
Mike.Cartwright@Pirean.com